20th International Conference on Structural Mechanics in Reactor Technology (SMiRT 20)
Espoo, Finland, August 9-14, 2009
SMiRT 20-Division 7, Paper 1849

Results and Insights from Interim Seismic Margin Assessment of the Advanced CANDU Reactor™ (ACR™) 1000 Reactor

T. Ha, U. Menon, T. Ramadan, P. Santamaura and M. Elgohary

Atomic Energy of Canada Limited 2251 Speakman Drive, Mississauga, Ontario, Canada, L5K 1B2, e-mail: hat@aecl.ca

Keywords: ACR-1000, CANDU, Seismic Margin Assessment, HCLPF, Severe Core Damage.

1 ABSTRACT

The ACR-1000™ reactor developed by Atomic Energy of Canada Limited (AECL) is a 1200-MWe-class-light water-cooled, heavy-water-moderated pressure-tube reactor, which has evolved from the well-established CANDU™ line of reactors. It retains the basic, proven, CANDU design features while incorporating innovations and state-of-art technologies to ensure fully competitive safety, operation, performance and economics.

The objective of this paper is to describe the seismic margin assessment (SMA) performed for the ACR-1000 reactor at full power operation. The ACR-1000 reference design basis earthquake (DBE) is 0.3g peak ground acceleration (PGA). The seismic margin was assessed, and potential seismic failure modes as well as weak component links/functionality leading to sever core damage and widespread fuel damage were identified.

The Level I internal event at-power PSA models were reviewed and the systems required to bring a plant from a normal operation to a safe shutdown were identified in the seismic safe shutdown equipment list (SSEL). In the first approach, seismic capacities of the items on the SSEL have been developed using the ACR seismic design criteria and qualification criteria, past seismic experience and recent seismic probabilistic safety analyses and seismic margin assessments. The plant responses to seismic events were modelled in seismic event trees, from which the accident sequences potentially leading to severe core damage and widespread fuel damage were identified. These accident sequences determined a combination of the failures of frontline safety systems. There are dependencies between frontline systems and their support systems, and among support systems. These dependencies were included appropriately using system dependency matrices. Then, the accident-sequence seismic capacities were estimated from the seismic failures of structures or components resulting in failures of frontline systems and their support systems in terms of high confidence of low probability of failure (HCLPF). The plant HCLPF capacities for severe core damage and widespread fuel damage were then determined.

This assessment demonstrates that the ACR-1000 design can reasonably achieve a seismic margin in terms of the plant HCLPF that is equal to or exceeding 0.5g PGA. Therefore the ACR-1000 design is capable of safe shutdown in response to a strong magnitude earthquake.

2 INTRODUCTION

The safety approach used for the ACR-1000[1] design gives a high prominence to reliability and Probabilistic Safety Assessment (PSA) studies. The PSA for ACR-1000 design was conducted during the plant design phase. Having these two activities progressing in parallel, allows for early implementation of the PSA insights in the plant design before construction. This reduces the risks and expenses of design modifications later in the project.

The SMA was conducted as a part of Level 1 PSA in support of the pre-project review of a two-unit ACR-1000 nuclear power plant, to assess the seismic margin for the ACR-1000 reactor following seismic

[1] ACR-1000™ (Advanced CANDU Reactor™) is a trade-mark of Atomic Energy of Canada Limited (AECL).

events at full power operation. This is a method consistent with the US NRC margin method described in NUREG-1407 [1] and SECY-93-087 [2]. According to the methodology, all seismic failure modes and component weak links/functionalities are considered. The ACR-1000 reactor is designed for a DBE of 0.3g PGA. The assessment should demonstrate that the ACR-1000 design meets the safety objective of a plant high confidence (95%) of low probability (5%) of failure capacity equal to or exceeding 0.5g PGA. The safety objective of 0.5g is calculated based on the accepted practice of selecting 1.67 times the DBE. This is equivalent to showing that no simple combination of seismic failures, each with HCLPFs less than 0.5g, can result in severe core damage or widespread fuel damage.

SMA methodology assesses the potential risk following seismic events in terms of plant HCLPF. For the SMA, seismic fault tree analysis and accident sequence quantification with event trees was not performed. Instead, system dependency matrices are used to derive accident sequence HCLPF capacities. A PSA-based SMA is presently being conducted including the development of seismic fault trees.

3 ACR-1000 DESIGN CONCEPT

The ACR-1000 reactor developed by AECL is a 1200-MWe-class-light water-cooled, heavy-water-moderated pressure-tube reactor, which has evolved from the well-established CANDU[2] line of reactors. Fig. 1 shows the general overview of the ACR-1000 design. It retains the basic, proven, CANDU design features while incorporating innovations and state-of-art technologies to ensure fully competitive safety, operation, performance and economics.

The major innovation in the ACR-1000 design is the use of low enriched uranium fuel and light water coolant. The ACR-1000 plant is a four quadrant design (for easier maintenance and improved reliability). There are five safety systems; (i) two independent, diverse and fast acting shutdown systems (SDS1 and SDS2), which are physically and functionally independent from each other and from the reactor regulating system; (ii) emergency cooling system; (iii) emergency feedwater system; and (iv) containment system, which includes a strong steel-lined containment structure. Another design feature is the reserve water system that supplies water for beyond design basis accidents (See Fig. 1).

The ACR-1000 design principle is to prevent and mitigate severe accidents and to reduce severe accidents consequences. It is based on a five-level defence-in-depth (DID) principle. The DID concept is applied to all safety activities, such that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the DID concept throughout design and operation provides a graded protection of normal operation against a wide variety of transients; anticipated operational occurrences; design basis accidents; and beyond design basis accidents including those resulting from equipment failure or human errors within the plant as well as external events. There are five levels of defence as per Canadian Nuclear Safety Commission (CNSC) Regulatory Document (RD-337) [3], including prevention, mitigation, control of plant conditions, reduction of consequences, and finally mitigation of radiological consequences.

3.1 Seismic Design Features

The seismic design philosophy implemented in the ACR-1000 design is based on requirements and criteria established by the CNSC [3] and the IAEA [4], to ensure the integrity and operability of the structures, systems, and components (SSCs) in the event of an earthquake. These requirements and criteria are formalized in CNSC RD-337, CSA N289 series [5], the IAEA guidelines [6-7], and the NBCC [8].

One of the key features in the safety system design in the ACR-1000 reactor is four-quadrant philosophy as shown in Fig. 2. That is, the SSCs important to safety will be physically and functionally separated. This is implemented in the seismic design of safety systems and safety support systems. The SSCs required to perform or support the performance of safety functions during and/or following an earthquake are seismically qualified. Those SSCs include the systems essential to shut down the reactor, maintain the heat transport system (HTS) coolant boundary and reactor core cooling, achieve containment isolation and heat removal, and to perform post-accident monitoring. Per four quadrant principle, each division (or quadrant) in safety support systems serves exclusively that pertinent division in frontline safety systems. Therefore, each division in frontline/support systems is functionally independent.

[2] CANDU™ (CANada Deuterium Uranium) is a trade-mark of Atomic Energy of Canada Limited.

The ACR-1000 design has two redundant reactor shutdown systems: SDS1 and SDS2. The SDS1 has 37 carbon carbide-filled shutoff rods, and the reactor shutdown can be achieved by automatically inserting these rods into the core by a trip logic system. The SDS2 uses the injection of neutron-absorbing solution into the moderator through horizontal nozzle assemblies. They are both seismically qualified and each implements the independent and functionally separated instrument and control logic.

The reactor coolant pressure boundary is seismically qualified. It includes the fuel channels, headers, pumps, pressurizer, steam generators, isolation valves on the pressure boundary, and/or connected subsystems, and supporting structures, moderator system, and calandria assembly/vault.

For residual heat removal, the ACR-1000 design has several safety systems. The emergency core cooling system and reserve water system in the primary side and emergency feedwater system and reserve water system in the secondary side. The reserve water system has a sufficient inventory for a mission time of 24 hours and is capable of supply emergency water makeup to reactor headers and steam generators even on total loss of Class III power including essential diesel generators. The uninterruptible power supply can provide electric power to the motorized valves in the distribution line and thereafter an inventory makeup can be established in a passive manner.

The barrier to radioactive release (e.g., containment) is also seismically qualified to maintain its liner integrity. The containment system includes containment isolation, containment cooling and its support systems. In addition, structures or components outside the containment envelope whose failure could result in the release of radioactive material other than in the reactor core and dose limits being exceeded are also seismically qualified. This includes the equipment in the spent fuel storage bay.

The control and motoring systems associated with the essential seismically qualified safety systems are all qualified for operation from the main control room (MCR) and secondary control area (SCA) following an earthquake. Should the MCR become unavailable, sufficient seismically qualified monitoring and control equipment is provided in the SCA to maintain the plant in a safe state, including the path operators need to take in a seismic event from MCR to SCA. Both MCR and SCA are seismically qualified.

To support these frontline safety systems, the ACR-1000 design has the supporting systems that are seismically qualified. These include essential electrical distribution system with four essential diesel generators that can be loaded to their dedicated bus, essential cooling water and essential service water systems, essential instrument air system that has four seismically qualified banks of instrument air bottles. As well, fire water supply system for water makeup to key loads, heating, ventilation and air conditioning system are seismically qualified. Seismically qualified batteries can supply backup power to the Class I buses and Class II conversion equipment for specified lengths of time (e.g., up to 24 hours for severe accidents) following an interruption to normal (Class III) source. The four-quadrant principle is implemented in design of these frontline systems and their support systems.

Before the plant is operational, an adequacy of ACR-1000 seismic design will be confirmed by a plant walkdown that is conducted by a multidisplinary team. It will assess the as-built condition of installed equipment, ensure they are capable of withstanding a DBE event. Significant emphasis in the walkdown is placed on the assessment of the as-build configuration, seismic interaction between SSCs, and anchorage features of equipment.

4 SEISMIC MARGIN ASSESSMENT APPROACH

The ACR-1000 SMA basically follows the PSA-based SMA methodology [9] except for performing the accident sequence quantification via seismic fault trees linking to seismic event tree models. It is intended to demonstrate seismic margin beyond DBE.

The SMA involves the following major steps; (i) identification of the SSCs required for safe shutdown following a seismic event (i.e., seismic safe shutdown equipment list (SSEL)); (ii) evaluation of seismic capacities of the items on the SSEL (i.e., fragility analysis); (iii) accident sequence HCLPF analysis (e.g., identification of seismic initiating events (IEs), seismic event tree analysis, and accident sequence HCLPF derivation).

Two broad categories of reactor damage states are defined in the PSA for ACR-1000 plant: widespread fuel damage and severe core damage. The widespread fuel damage accidents affect the core that result in fission product release due to fuel overheating, but do not result in consequential pressure tube failures. The

severe core damage is the condition where there is extensive physical damage to the core such that fuel bundles and channels would be disassembled either by mechanical damage or by melting. Onset of severe core damage occurs when the moderator fails to effectively remove the heat from the fuel channels in the accident sequence involving degradation of fuel cooling.

5 SEISMIC SAFE SHUTDOWN EQUIPMENT

The SSCs that are required to bring the plant to a safe shutdown condition following seismic events need to be identified in the SSEL. The Level 1 internal events at-power PSA models (e.g., event tress and fault trees) are reviewed and the systems credited are identified. These are the systems important to safety that are required to bring the plant from a normal operation condition to a safe shutdown condition, to ensure safety during and following seismic events. They include both frontline systems and their support systems. The support systems (e.g., electrical power, cooling water, instrument air, etc.) provide services to the frontline systems. The critical components are identified and included in the SSEL from the review of the appropriate design documents for these systems. Some passive components (e.g., piping) that are not explicitly modelled in system fault trees are added. Since the Level 1 PSA models do not provide a complete list of SSCs for the SMA, several items should be added in the SSEL such as structural items (e.g., electrical panels and cabinets, walls, etc.) and structures (e.g., reactor building, reactor auxiliary building, etc.) that house the critical components identified in the SSEL. The SSEL also includes items that may fail during an earthquake and that may lead to a seismic induced IE.

6 FRAGILITY ANALYSIS

The ACR-1000 reactor is being designed as per the seismic design requirements (as specified in Section 3.1). Because of the conservatisms inherent in seismic design and qualification procedures, the actual seismic capacities of the seismically qualified structures and equipment will be higher than the DBE. Such conservatisms arise from the following sources:

- Definition of the DBE input ground motion.
- Seismic response calculation of structures important to safety and generation of design floor response spectra.
- Acceptance criteria of structures and equipment; e.g., load combinations, stress limits, and qualification testing.

The plant-specific seismic capacities can only be determined after the seismic design is complete, and the structures and equipment installation is implemented. As such, seismic capacities for structures and equipment that have their design finalized are calculated. For the remainder of structures and equipment, their capacities are estimated based on the ACR-1000 seismic design criteria, generic data, as well as past seismic PSA and margin assessments.

The ACR-1000 SSCs are judged to be conservatively designed based on the review of the seismic requirements and the DBE ground motion, such that significant margins beyond the design basis are expected. A probabilistic approach is taken to estimate the median (best estimate, Am) capacity of each component, as well as its composite variability (βc). The median capacity and composite variability are estimated using a combination of ACR-1000 design criteria, seismic PSA and SMA experience as part of recent advanced reactor design certifications. It is to be noted that the median capacity may still be a conservative estimate, since the actual design may have additional margins, which are not accounted for here. The HCLPF capacity of the components is derived using these values: $HCLPF=Am\cdot\exp(-2.33\beta c)$. Then the median seismic capacity, Am, and the associated composite variability, βc, and the HCLPF capacity in terms of PGA are provided for the SSEL items for the ACR-1000 reactor.

The objective of the SMA is to show that the ACR-1000 design has inherent seismic margin and that it is reasonable to expect the HCLPF capacity of the plant to exceed 0.5g PGA. For this purpose, a screening HCLPF value of 1.0g is proposed. The components with HCLPF capacities more than 1.0g PGA are screened out, whereas those with HCLPF capacities less than 1.0g are further assessed and are included in the model.

One of the novel features of the ACR-1000 project is the way feedback from the SMA is incorporated in the design process to ensure that the seismic safety objectives are met. This carried out in several steps. The first step is to include the minimum fragility requirements from the SMA in the design requirements of the SSC's that are identified in the SSEL. The second step is that after the detailed design is completed, detailed fragility calculations are performed to confirm that the requirements are met. The third step is that after the construction is essentially completed, the pre-operational seismic walkdown (see section 3.1) is carried to confirm that the plant is built as designed.

7 ACCIDENT SEQUENCE ANLAYSIS

The SMA evaluates the risk associated with seismic initiators by determining whether there is adequate margin above the DBE (0.3g). Scenarios in which combinations of seismic failures and non-seismic failure events could result in a seismic capacity less than the safety objective capacity of 0.5g are identified.

For this evaluation, the initiating events and event trees in Level 1 internal at-power PSA are reviewed to identify which events need to be included in the seismic model. Then seismic event trees are constructed to model the plant response following seismic events. Without performing seismic system fault tree analysis, two system dependency matrices are constructed to incorporate the dependency between frontline systems and their support systems, and the dependency among support systems in the ACR-1000 design. These dependencies should be appropriately included in the accident sequence HCLPF evaluation. The "MIN-MAX" method is used to evaluate accident-sequence HCLPF capacities at the accident sequence level and the plant-level HCLPF capacity. The MIN-MAX method assesses the accident sequence HCLPF by taking the lowest HCLPF value for components analyzed under OR-gate logic and the highest HCLPF value for components analyzed under AND-gate logic. This evaluation provides identification of the structures and equipment that lead to severe core damage, which determines the plant-level HCLPF. The HCLPF results and PSA insights from this evaluation are assessed to identify potential seismic vulnerabilities relative to safety objective HCLPF capacity of 0.5g.

7.1 Assumptions

The key assumptions for the ACR-1000 SMA are listed:

- The seismic event is assumed to occur while the plant is operating at full power.
- It is assumed that the seismic event would result in loss of off-site power (e.g., loss of Class IV power).
- No credit is taken for non-seismically qualified SSCs. They are assumed to have failed or to be non-functional due to seismic event.
- The ACR-1000 plant uses solid-state switching devices and electromechanical relays in the instrumentation and control (I&C) systems. Solid-state switching devices are known to be inherently immune to the contact chatter. When used, electro-mechanical relays of robust seismic capacity will be selected to preclude the concern for seismic induced relay chatter.
- The ACR-1000 plant has been designed such that the sources of potential seismic induced fire and flooding interactions are minimized. Therefore they are not included in this assessment. Before the plant is operational (i.e., when the plant is substantially completed), however, a seismic walkdown will be conducted to confirm the assumption.

7.2 Identification of Seismic Initiating Events

There is only one initiator for the SMA. That is a seismic event whose magnitude is large enough to demonstrate that the ACR-1000 design has sufficient margin above the design basis level earthquake. The level of the seismic event may vary, but the structure of the accident sequences describing plant response to seismic events of these various levels can be represented by the same set of event trees. Only failure probabilities vary with seismic level.

As a result of seismic event, plant equipment may be damaged (e.g., leading to a small loss of coolant accident (LOCA)), requiring different combinations of plant system responses to achieve a safe plant shutdown. The initial plant equipment damage may be equivalent to one or more initiators already modelled

in the Level 1 internal events at-power PSA. The major difference for seismic margin assessment is that more than one such damage or "initiator" caused by the seismic event is considered simultaneously as appropriate. The seismic failures of several structures or equipment are identified as potentially seismic-induced initiators. These initiators may result directly in severe core damage and therefore they need to be considered separately.

To take advantage of the work already performed for the Level 1 internal events at-power PSA for the ACR-1000 reactor, the IEs are reviewed to determine whether or not they need to be treated as seismic induced initiators. Some IEs are considered as seismic induced imitators in seismic models such as small LOCA due to out of core failures, heat transport system large LOCA, etc. Some other IEs are not considered seismic initiators but are considered in plant response model to seismic event, such as loss of end shield heat sink, loss of plant instrument air system, etc.

7.3 Seismic event tree

Two sets of event trees are developed. The first set is the seismic pre-tree with nine groups of seismic induced failures of structures and equipment as top events. The pre-tree and the definition of the top events are shown in Fig. 3. This tree is used to track the sequences needed to identify unique seismic failures. The sequences in the seismic pre-tree terminate in either reactor damage sate in which reactor core has partially or fully dissembled, or some seismic induced IEs. The event order in this pre-tree depends on the results of seismic capability of the systems. For this study, a seismic induced failure of loss of off-site power is assumed for all sequences. It is expected to occur at relatively low level of ground motion; i.e., well below the seismic motions considered in this assessment. This is equivalent to assuming an initial total loss of class IV power, which disables the systems that are powered from class IV electrical distribution system; e.g., main feedwater pumps, heat transport system pumps, etc. Ten seismic sequences are identified from the pre-tree. These sequences represent seismic failures that may lead directly to a pre-defined reactor damage states or to three additional seismic induced initiating events that require different plant response for mitigation.

The second set of seismic event trees is then developed for these three seismic induced initiating events (e.g., no LOCA, small LOCA, and large LOCA seismic events). Level 1 internal events at-power PSA models are modified considering seismic-induced plant conditions. No LOCA seismic event tree models the plant response when there is a loss of class IV power but no LOCA present. Small LOCA seismic event tree models the plant response when a small LOCA is present with a loss of class IV power. Large LOCA seismic event tree models the plant response to a large LOCA with a loss of class IV power.

8 RESULT

The accident sequences leading to the predefined reactor damage states are identified from seismic event trees. A combination of the failures of the frontline systems for each sequence that can lead to severe core damage or widespread fuel damage is determined. Functional dependency between frontline systems and their support systems, and among support systems, is addressed in accident sequence HCLPF evaluation from two dependency matrices. The seismic failures of structures or components that lead to the failures of these systems are combined to evaluate each accident-sequence HCLPF capacity using MIN-MAX method.

Each accident sequence identified is then categorized as severe core damage or widespread fuel damage based on its definition. From the set of accident-sequence HCLPF capacities in each category, the plant HCLPF for severe core damage and widespread fuel damage are determined using MIN-MAX approach. The result is summarized in Table 1. The assessment results indicate that the plant HCLPF for both severe core damage and widespread fuel damage considering only seismic-induced failures is equal to or exceeds 0.5g PGA.

The accident sequences leading to severe core damage are analyzed. The most significant HCLPF sequences are involved with seismic induced failures of both main control room and secondary control area functionalities (e.g., control panels, operator consoles, etc.) or seismically qualified electric power (Class I/II/III) supply system, or seismically qualified I&C cabinets (e.g., protection logic, control logic, and monitoring system), or both reactor shutdown systems.

For widespread fuel damage, the most significant sequences involve the seismic induced failures of seismically qualified I&C cabinets.

Table 1 ACR-1000 Plant HCLPF Capacities.

End states	Plant HCLPF capacity
Severe Core damage	0.5g
Widespread fuel damage	0.5g

9 CONCLUSION

The ACR-1000 reactor is designed to be capable of safe shutdown in response to a DBE (0.3g). The seismic margin assessment demonstrates that the ACR-1000 design can reasonably achieve a seismic margin measured in terms of the plant HCLPF that is equal to or exceeding 0.5g PGA for both severe core damage and widespread fuel damage.

REFERENCES

[1] Chen et al. 1991. Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities, NUREG-1407, US NRC.

[2] SECY-93-087. 1993. Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactors (ALWRs) Designs, US NRC.

[3] Canadian Nuclear Safety Commission (CNSC). 2008. Regulatory Document RD-337, Design of New Nuclear Power Plants

[4] IAEA NS-R-1. 2000. Safety of Nuclear Power Plants: Design

[5] Canadian Standards Association. CSA N289.1. 2008. General Requirements for Seismic Design and Qualification of CANDU Nuclear Power Plants

[6] IAEA NS-G-3.3. 2002. Evaluation of Seismic Hazards for Nuclear Power Plants, Vienna.

[7] IAEA NS-G-1.6. 2003. Seismic Design and Qualification for Nuclear Power Plants, Vienna.

[8] National Research Council Canada. 2005. National Building Code of Canada.

[9] US NRC. 1986. NUREG/CR-4482, Recommendations to the Nuclear Regulatory Commission on Trial Guidelines for Seismic Margin Reviews of Nuclear Plant Plants: draft report for comment

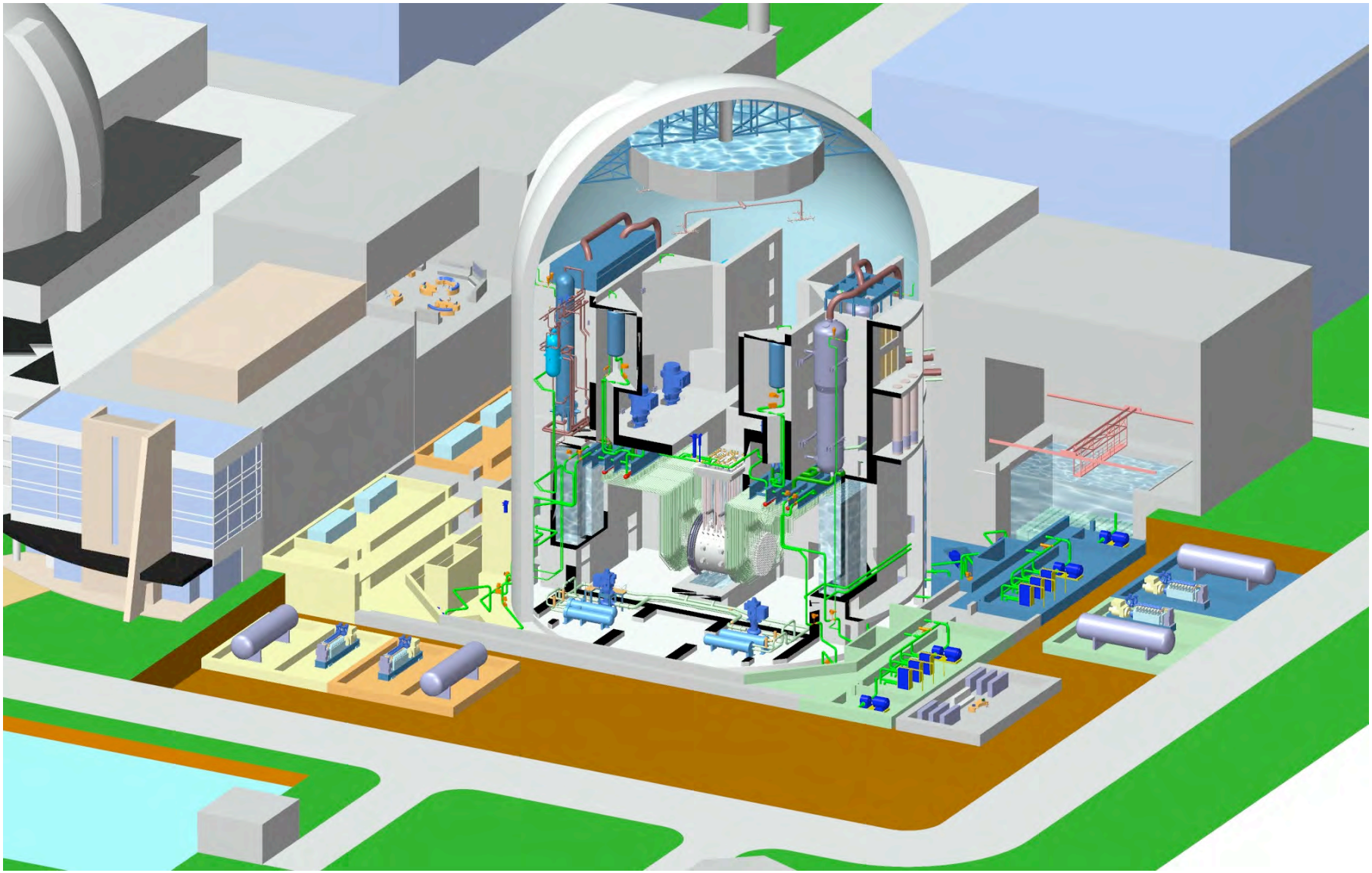

Figure 1. ACR-1000 Design Overview

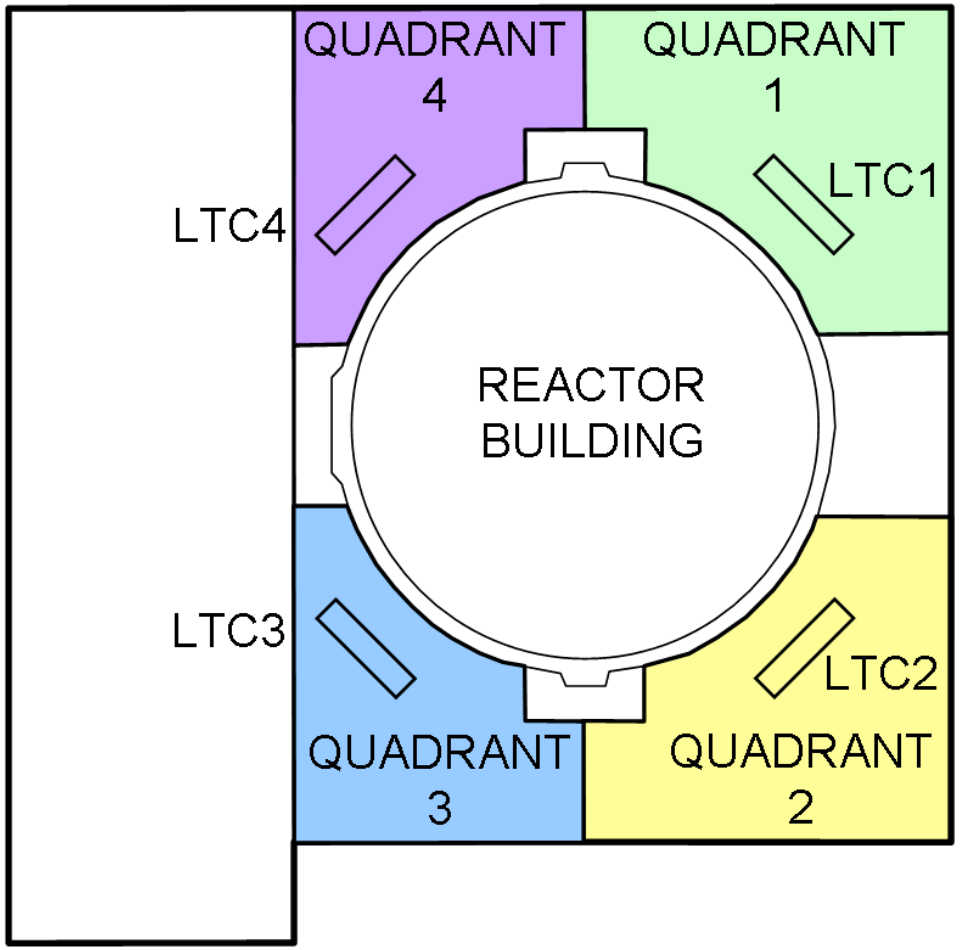

Figure 2. Four-Quadrant Philosophy for Design of Safety Systems and Safety Support Systems in the ACR-1000 Design

IE-EQSMAM1	NBYPASS	STRUC	NELOCA	RS	NEPS	NFM	NLLOCA	NSLOCA	SGPR	Plant Damage State	Sequence Label
Earthquake	No Containment Bypass	Structural Integrity	No Excessive LOCA	No Reactor Shutdown by SDS1 or SDS2	No Electric Power (CL. I/II/III)	No Fuel Channel Ejection	No Large LOCA	No Small LOCA	SG Pressure Relief		
Initiating Event	Seismic	Seismic	Seismic	Reactor Shutdown	Seismic	Seismic	Seismic	Seismic	Seismic		

Figure 3. ACR-1000 Seismic Pre-tree